The Division Algorithm for $\mathbb{N}$ and $\mathbb{Z}$

Theorem (Division Algorithm for $\mathbb{N}$) Suppose a and b are natural numbers and that $b \leq a$. Then there is a natural number q and a whole number r such that $a = bq + r$ and $0 \leq r < b$. Moreover, q and r are unique.

(*We usually call q the "quotient" and r the "remainder" when a is divided by b.*)

Proof Let $A = \{s \in \mathbb{N} : sb > a\}$. There must be at least one such value of s (*see the "Archimedean Principle", text, p. 105*), so $A \neq \emptyset$. By the Well-Ordering Principle (WOP), A contains a smallest element: call it l.

Since $1 \notin A$, we know that $l > 1$ so $q = l - 1$ is a natural number. Define $r = a - bq$. This makes $a = bq + r$. (*But we still need to prove that* $0 \leq r < b$).

We know that $\begin{cases} lb > a & \text{because } l \in A \\ (l-1)b = qb \leq a & \text{because } q < l \text{ and therefore } q \notin A. \end{cases}$

Since $qb \leq a$, we have $r = a - bq \geq 0$.

To see that $r < b$: if $r = a - bq \geq b$, we would have
$a \geq b + bq = b + b(l-1) = lb$, which is false.

Therefore $0 \leq r < b$ so the proof "there exist" q and r with the desired properties is complete

To prove q and r are unique: Suppose $a = bq + r$ where $0 \leq r < b \quad (*)$
and that $a = bq' + r'$ where $0 \leq r' < b \quad (**)$

Subtracting these equations and rearranging gives $b(q - q') = r' - r$, and therefore

$$b|(q - q')| = |r' - r|. \qquad (***)$$

Also, we know from $(*)$ that $-b < -r \leq 0$, and adding this inequallity to the inequality
$0 \leq r' < b$ $(**)$ gives
$-b < r' - r < b$ so that

$$|r' - r| < b$$

Substituting this in $(***)$, we get $b|(q - q')| < b$.

This means that $|q - q'| < 1$ and, since $|q - q'|$ is a integer, this implies that $|q - q'| = 0$, that is, $q = q'$. From this, and the equations

$$a = bq + r$$
$$a = bq' + r'$$

we get that $r = r'$. Therefore q, r are unique. •

(*over* $\rightarrow$)

We can also state a division algorithm for $\mathbb{Z}$.

Theorem (Division Algorithm for $\mathbb{Z}$) Suppose a and b are integers and that $b > 0$
Then there is an integer q and an integer r such that $a = bq + r$ and $0 \leq r < b$.
Moreover, q and r are unique.

There are various ways to state the division algorithm for $\mathbb{Z}$. In this version, we require that the divisor $b > 0$, so actually $b \in \mathbb{N}$, and that $0 \leq r < b$. Another version (you might try to prove it) allows b to be any nonzero integer and has $0 \leq r < |b|$. In all versions, the statement requires that the remainder r be nonnegative: that fact is usually what's important when the Division Algorithm is used.

Proof If $a > 0$, we get q and r from the Division Algorithm in $\mathbb{N}$.
If $a = 0$, let $q = r = 0$.
If $a < 0$, then apply the Division Algorithm in $\mathbb{N}$ for dividing $-a$ by b. There are natural numbers q' and r' for which

$$-a = bq' + r' \qquad \text{where } 0 \leq r' < b$$

Then $a = b(-q') - r'$ where $-b < -r' \leq 0$.

Using this equation:

Case i) If $-r' = 0$:

Let $q = -q'$, $r = 0$. Then $a = b(-q') - r' = bq + r$ where $0 \leq r < b$

Case ii) If $-b < -r' < 0$:

Let $q = -q' - 1$ and $r = b - r'$.

$$\begin{aligned} \text{Then } a = b(-q') - r' &= b(-q') - b - r' + b \\ &= b(-q' - 1) + (b - r') \\ &= bq + r, \quad \text{where } 0 < b - r' = r < b \\ &\qquad\qquad\qquad\qquad \text{(since } -b < -r' < 0\text{).} \end{aligned}$$

So, in both cases, we can find integers q and r for which $a = bq + r$, with $0 < r < b$.

The proof that q and r are unique is left as an exercise (*see proof of the previous theorem for ideas*). •

Example The division algorithm in $\mathbb{N}$: $3 < 7$ so we can write $7 = 3q + r$ where $0 \leq r < 2$
(namely, with $q = 2$ and $r = 1$)

The division algorithm in $\mathbb{Z}$ (in the form stated above, requiring the divisor $b > 0$) with $b = 3$ and $a = -7$ says that we can write $-7 = 3q + r$, where $0 \leq r < 3$. Here the values that work are $q = -3$ and $r = 2$, and that's the <u>only</u> way to pick q and r if you want $0 \leq r < 3$.

We proved the Division Algorithm for $\mathbb{N}$ using WOP. Here's an alternate proof using PMI, doing "induction on b." Stated more formally, we want to prove:

$$(\forall b \in \mathbb{N})(\forall a \in \mathbb{N})(\exists q \in \mathbb{N})(\exists r \in \mathbb{N}) \ \ (a = bq + r) \wedge (0 \leq r < b)$$

To prove this universal statement (working left to right), we pick any $b \in \mathbb{N}$.

For this arbitrary but fixed natural number b we need to prove that

$$(\forall a \in \mathbb{N})(\exists q \in \mathbb{N})(\exists r \in \mathbb{N}) \ \ (a = bq + r) \wedge (0 \leq r < b)$$

This is a statement of the form $(\forall a \in N)\, P(a)$, where $P(a)$ is the statement

$$(\exists q \in \mathbb{N})(\exists r \in \mathbb{N}) \ \ (b = aq + r) \wedge (0 \leq r < a)$$

We use induction on the natural number a.

This looks just a little odd, but a is a natural number, so induction is OK; if it makes you more comfortable, change "a" everywhere to "n."

Proof Base case: Suppose $a = 1$.

If $b = 1$, let $q = 1$ and $r = 0$. Then $a = bq + r$ and $0 \leq r < 1$
If $b > 1$, let $q = 0$ and $r = 1$. Then $a = bq + r$ and $0 \leq r < 1$.
So $P(1)$ is true.

Induction step: Suppose $P(a)$ is true for some particular value of a. Thus, we are assuming (for this value of a) that there are natural numbers q' and r' for which $a = bq' + r'$ and $0 \leq r' < b$.

We need to prove that $P(a + 1)$ is true, that is, that there exists natural numbers q and r for which $a + 1 = bq + r$, where $0 \leq r < b$.

Case i: If $r' = b - 1$: $\quad a = bq' + r' = bq' + b - 1$, so
$a + 1 = bq' + b \ = b(q' + 1) + 0$

Let $q = q' + 1$ and $r = 0$
Then $a + 1 = bq + r$, where $0 \leq r < b$

Case ii: If $r' < b - 1$: $\quad a = bq' + r'$ so
$a + 1 = ab + (r' + 1)$

Let $q = q'$ and $r = r' + 1$
Then $a + 1 = bq + r$, where $0 \leq r < b$.

In both cases, we can find the necessary q and r. So $P(k + 1)$ is true.

By PMI, $(\forall a \in \mathbb{N})\ P(a)$ is true (for the particular b we chose). Since the argument works no matter which $b \in \mathbb{N}$ we choose, we conclude that

$$(\forall b \in \mathbb{N})(\forall a \in \mathbb{N})(\exists q \in \mathbb{N})(\exists r \in \mathbb{N}) \ \ (a = bq + r) \wedge (0 \leq r < b) \quad \bullet$$